

Can Laws Block Spam?

An analysis of the effect of international spam legislation

www.vircom.com



© 2004 Vircom, Inc. All rights reserved.

Introduction

The massive amounts of unsolicited commercial e-mail (spam) that have choked inboxes worldwide for the past few years have created a very rare occurrence amongst some of the world's political powers: Agreement!

Not only agreement, but action - The United States, the European Community, Australia and the United Kingdom have all recently implemented legislation regulating the control and handling of unsolicited commercial e-mails.

The complexity of this issue and the widely divergent approaches being used to address the spam problem are apparent in the different legislative approaches that these countries have used. However the question still remains...

Can spam ever be controlled through legislation?

That is the million-dollar question that legislators, analysts, and every consumer with an electronic mailbox are wondering.

© 2004 Vircom, inc. This white paper is the exclusive property of Vircom, inc. Distribution, reproduction or deletion, in whole or in part, of this document is strictly prohibited without prior written consent from Vircom.

Modus, Modus3, ModusMail, ModusGate, Sequential Content Analyzer, SCA, are all trade marks of Vircom, inc. All other products or services mentioned in this document are identified by the trademarks or service marks of their respective companies or organizations. Complete legal statements are available at <http://www.vircom.com/Corporate/Legal.asp>

Acknowledgements

In order to shed some light on the issue of anti-spam legislation, we looked at three recent anti-spam laws passed in The United States, The United Kingdom and Australia, and analyzed both the positive and negative aspects of these laws.

In addition, we consulted several of the foremost experts on the issue of spam for their views on these laws as well as whether or not legislation could ever stem the tide of spam.

This analysis would not have been possible without the views and opinions of these leading anti-spam experts who contributed to this document. Vircom wishes to acknowledge their invaluable contribution and shows unconditional support to the organizations that each of them represents.

Contributing experts

Lindsay Barton

Manager, Online Policy at the National Office for the Information Economy of Australia
<http://www.noie.gov.au/projects/confidence/Improving/spam.htm>

Anne P. Mitchell, Esq.

President/CEO, Institute for SPAM and Internet Public Policy
Professor of Law, Lincoln Law School of San Jose, California
<http://www.isipp.com>

Michael D. Osterman

President and Founder, Osterman Research
www.ostermanresearch.com

Troy Rollo

Chairman of the Coalition Against Unsolicited Bulk Email in Australia
Executive Director of the International Coalition Against Unsolicited Commercial Email
<http://www.cauce.org.au/>

Neil Schwartzman

Editor & Publisher spamNEWS,
Chair, Canadian Coalition Against Unsolicited Commercial Email
www.spamnews.com

The Radicati Group
estimates
the overall cost
of spam in 2003
to be in excess of
\$20.5 billion
worldwide.

The Need for Anti-Spam Legislation

The costs of spam

The concern about spam is growing and well-founded. Spam is estimated to make up over 65 percent of all e-mail traffic today, perplexing and harassing consumers, enterprises, internet service providers and legitimate e-mail marketers alike. The Radicati Group has estimated the overall cost of spam in 2003 to be in excess of \$20.5 billion worldwide.

Consumers are deluged daily with mailboxes full of messages for online prescriptions, low interest loans, or the latest weight loss product, some e-mail messages are just simply annoying, while others border on the offensive or illegal.

Enterprises are subject to lost productivity, soaring bandwidth consumption, increased storage costs as well as fear of legal liabilities and responsibilities towards their employees. Osterman Research has estimated that the economic cost of spam is \$1,400 a year for every enterprise e-mail user. For a company of only 10 employees, this represents an additional cost of \$14,000 per year all due to spam.

Spam results in higher costs for Internet Service Providers with reduced bandwidth, increased storage and personnel costs as well as complaints and possible loss of reputation from clients.

Legitimate e-mail marketers are burdened with adjusting and readjusting their business practices to comply with changing regulations, as well as being challenged with the devaluation of their product or service because of spam and the stigma of being associated with spammers.

"E-mail has become the major delivery mechanism for marketing material simply because of dollars and cents," says Michael D. Osterman. "Whereas other marketing strategies like bulk mail involve costs to create, produce and send the material, the cost of sending spam is virtually non-existent."

Michael D. Osterman

Osterman Research
has estimated
that the economic
cost of spam
is \$1,400 a year
for every enterprise
e-mail user.

Current Anti-spam legislation

The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 - CAN SPAM Laws in the United States Regulating Spam

After years of debate and arguments, the United States enacted legislation designed specifically to curb the flood of spam. The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act) went into effect on January 1, 2004 establishing a national law governing e-mail spam, which currently makes up more than two-thirds of all e-mail messages in circulation.

According to The United Nations Conference on Trade and Development (UNCTAD) 2003 e-commerce and development report currently over 58% of all e-mail spam originates from the United States. The United States therefore must take on the role of having to be the world's leader in policing spam.

CAN-SPAM: A Compromised Solution

CAN-SPAM represents a compromise amongst all concerned with the growing rate of unsolicited commercial e-mails, including: Internet service providers, e-commerce businesses, enterprises, consumer groups as well as the direct marketing lobby.

Opt-Out Provision

The most controversial issue regarding the CAN-SPAM act is the requirement that each commercial electronic message sender must provide a viable opt-out capability in every message. If the receiver decides to opt-out, the sender of the message must take that person off their list within 10 days and send a confirmation to the receiver to illustrate that they have been removed. The big concern regarding the opt-out mechanism is that it gives spammers the right to spam.

"The 'opt-out' provision will prove useless - even discounting the numerous technical difficulties associated with such a facility it is already literally impossible for many people to 'opt-out' of the volume of spam they get now," explains Troy Rollo. "In addition despite common misconceptions about the law, it simply does not ban harvesting - the anti-harvesting provision only applies where the spam is already illegal for other reasons - nor does it create an effective 'do not email' list - there is no provision in the American law requiring compliance with such a list if it were created."

Troy Rollo

CAN-SPAM in Detail

CAN-SPAM prohibits both individuals and enterprises from distributing "predatory and abusive commercial e-mail messages." Specifically, the act outlaws sending multiple e-mail messages that contain false header information or that hijack unauthorized computers, domain names, or Internet protocol (IP) addresses to disguise their origins.

Hijacking computer systems

CAN-SPAM outlaws the unauthorized use of or hijacking of protected computer systems to: initiate, relay, and or retransmit any type of e-mail message. Spammers often distribute messages by hijacking third-party servers, allowing them to hide their origins and thus avoid being blacklisted or removed from the internet traffic by internet service providers.

CAN-SPAM
represents
a compromise
amongst all
concerned with
the growing rate of
unsolicited
commercial e-mails

Misleading header information

CAN-SPAM makes it unlawful for senders to transmit unsolicited commercial e-mail messages with headers containing false e-mail addresses, domain names, or Internet protocol (IP) addresses. The legislation requires the senders to identify themselves in the "From" line of the header.

In addition, CAN-SPAM also:

- Prohibits spoofing by having the sender include a valid return e-mail address or other means to respond to the message;
- Prohibits the use of deceptive subject headings;
- Requires the sender to include a valid postal address in e-mail messages;
- The message must also clearly be identified as an advertisement and or solicitation, and;
- It must inform recipients of their right to decline such messages.

False identities

CAN-SPAM prohibits individuals and enterprises from sending messages through e-mail or online user accounts or domain names that were obtained using false identities. It is considered unlawful for senders to falsely represent themselves as the owner and or user of the internet protocol addresses from which they send their messages.

In addition, CAN-SPAM makes it illegal to use automated techniques such as programming scripts to sign up for e-mail accounts for the purposes of sending unsolicited commercial e-mails. These types of techniques (whack-a-mole) enable a spammer to create new e-mail accounts easily, which then makes them more elusive to internet service providers.

Sexually-oriented material

CAN-SPAM requires senders of messages containing sexually explicit content to issue warning labels in the subject header or make such a warning clearly visible to the user when they open the message. The legislation gives authorization to the Federal Trade Commission to create identifiable labels that would be included in any sexually oriented messages.

Address harvesting

CAN-SPAM prohibits address harvesting and dictionary attacks. Many spammers use automated software, robots, and spiders to collect e-mail addresses throughout the internet by searching web sites, newsgroups, mail lists or other online resources that could possibly contain e-mail addresses. Dictionary attacks use software that automatically requests likely e-mail addresses by combining letters and numbers in an attempt to find or validate active e-mail addresses.

Enforcement

The principal authority used to oversee and enforce the CAN-SPAM Act would be the Federal Trade Commission (FTC). Individuals or businesses that violate the act are subject to fines, imprisonment, or both. The maximum civil penalty is \$1 million USD.

The legislation also provides various enforcement powers for certain related violations to:

- The Federal Communications Commission,
- The Securities and Exchange Commission,
- The Federal Reserve Board,
- The Federal Deposit Insurance Corporation,
- The Office of the Comptroller of the Currency,
- The National Credit Union Administration,
- The Office of Thrift Supervision,
- The Secretary of Transportation,
- The Secretary of Agriculture,
- The Farm Credit Administration.

"Do Not E-mail" Registry

Based upon the legislation for telemarketers regarding the 'do-not-call' registry, the 'do not e-mail' registry will work towards helping control the activities of spammers. When a complaint is received, the sender of the unsolicited commercial e-mail will receive a warning. Upon any other complaint, the sender will face possible penalties including fines, blacklisting or removal of website by the internet service provider. The Federal Trade Commission will oversee the implementation of the "do not e-mail" registry.

Overruling the Individual States

The CAN-SPAM Act supercedes anti-spam legislation enacted by many individual states, which in some cases, like California's S.B. 186, established more stringent guidelines for commercial e-mail and had far stricter penalties for violators. An individual state however may pursue civil cases in Federal court against spammers whose e-mail messages adversely affect residents of that state. States may also seek to obtain civil damages on behalf of its residents.

Can CAN-SPAM - Reduce SPAM?

The CAN-SPAM Act, as well as the short time frame between its adoption and its implementation on the first day of 2004, has created a fire storm of controversy as to its strengths and weaknesses.

Supporters of the CAN-SPAM Act note that it has taken the first concrete steps towards creating solid legislation to eliminate spam.

A Positive First Step

"Any law is only as good as its enforcement, and this is certainly true for the U.S.' CAN-SPAM. While many decry its potential at helping to fight spam, it actually provides law enforcement with some very sharp tools. If those tools are actually used and used well, there is certainly the potential to make a dent in spam," explains Anne P. Mitchell. "There is, of course, going to be no change until enforcement happens, so it is not a surprise that the day after the law went into effect on January 1, 2004, there was no change in the level of spam."

Anne P. Mitchell

"In all cases, this law as well as all the other anti-spam laws recently passed, are all important first steps that will be effective to a degree, but perhaps more importantly provide reference points against which we can measure, judge, review and learn from, in future efforts to create legal defenses against spam."


Neil Schwartzman

Detractors claim that the CAN-SPAM Act has created a safe haven for spammers, By effectively legalizing spamming.

Won't it Hurt the Spammers?

"I have looked carefully at this legislation and in its present form it is almost completely ineffective against all but the most egregious, high-profile spammers. Anti-spam legislation satisfies politicians hoping to please their constituents but they do very little to solve the problem they're intended to solve".

Michael D. Osterman



"Over time, the US legislation should make spammers be more honest about who they are, but it won't stop a single piece of spam. Since it merely prescribes certain things spammers must include in their spam, and requires them to provide an opt-out capability, after the law is enforced a few times American spammers will merely adapt to the new rules and continue spamming," explains Troy Rollo. "They will be joined by lots of new spam from merchants who have hitherto held back, but will move into the area seeing that rules have been prescribed, viewing this as an indication that it is legal. While it seems bizarre to rational people that anybody would construe the American law as "legalizing" or encouraging spam, we have seen spammers themselves claim this about the failed Senate Bill in 1988 (S.1618), and this is exactly what happened when Korea established a substantially similar law - spam from Korea increased by a factor of 11 within 3 months, which much of it coming from well-established and well-financed stores."

Troy Rollo

The Privacy and Electronic Communications Regulation 2003 (EC Directive)

Laws in the United Kingdom Regulating Spam

Beginning in 1990, several laws have been passed concerning the distribution of unsolicited commercial e-mails in the United Kingdom. However, it was not until December 11, 2003 that the current legislation, "The Privacy and Electronic Communications Regulation 2003 (EC Directive)", came into effect.

EC Directive in Details

Under the Privacy and Electronic Communications Regulation 2003 (EC Directive), Section 22 outlines the regulations regarding unsolicited commercial e-mails.

"A person shall neither transmit, nor instigate the transmission of unsolicited communications for the purpose of direct marketing by means of electronic mail unless the recipient of the electronic mail has previously notified the sender that he consents for the time being to such communications being sent by, or at the instigation of, the sender."

With the exception that "A person may send or instigate the sending of electronic mail for the purpose of direct marketing where:

- That person has obtained the contact details of the recipient of that electronic mail in the course of the sale or negotiations for the sale of a product or service to that recipient.
- The direct marketing is in respect of that person's similar products and services only
- The recipient has been given a simple means of refusing (free of charge except for the costs of transmission of the refusal) the use of his contact details for the purposes of such direct marketing, at the time that the details were initially collected, and, where he did not initially refuse the use of the details, at the time of each subsequent communication."

Enforcement

The regulations will be enforced by the Information Commissioner. The Information Commissioner's office has the power to investigate and issue enforcement notices to individuals or companies which breach the Regulations. Breach of an enforcement notice is a criminal offence liable to a fine of up to £5,000 if handled in a magistrate's court, or an unlimited fine if the trial is before a jury. In addition, persons who have suffered damages because the Regulations have been breached have the right to sue the responsible person(s) for compensation.

Can The EC Directive Reduce Spam?

Supporters of this Regulation praise its attempts to protect the consumers privacy regarding unsolicited commercial e-mail.

A Regulation for the people

The EC Directive attempts to save consumers time and headaches in dealing with the deluge of spam. It also attempts to regain consumers trust in electronic mail.

* Source: BBC News: <http://news.bbc.co.uk/2/hi/technology/3120628.stm>

...Persons who have
suffered damages
...have the right to
sue the responsible
person(s)
for compensation

A Regulation for the Internet Service Provider as well

The EC Directive attempts to answer the Internet Service Providers' needs by reducing the volume of unsolicited commercial e-mails clogging the internet, taking up unnecessary bandwidth.

Chief amongst the criticism of this new Regulation for detractors is that it does not take into account business-to-business commercial e-mails:

Only half a law

The anti-spam group, Spamhaus, has criticized the new law for excluding Business addresses. "Britain has disappointed the internet community by actually legalizing the spamming of British businesses," said a Spamhaus statement. "From 11 December it will be legal to send spam to the millions of hapless employees of British businesses. Britain's firms will continue to suffer the onslaught of ever more spam, now from spammers claiming legality." *

Troy Rollo also views the exemption of business-to-business commercial e-mails as a major flaw. "The UK law may stop some spam from the UK, but it has two problems. Firstly, while it does ban most categories of spam it has a blanket exemption for spam sent to businesses. This is unfortunate since businesses are generally in even more urgent need of relief from the burdens of spam than consumers. The exemption is likely to encourage a trade in lists of domain names used by businesses, as opposed to Internet Service Provider domains where a recipient may or may not be operating a business. Thus it may provide little to no relief for enterprises, who are suffering real and significant costs due to spam - for them, spam has become a real drain on the economy, sucking up labour and resources for no useful purpose."

Troy Rollo

In a report released in October of 2003 entitled "Spam", the All Party Internet Group also criticized the regulation for its exclusion of business-to-business spam: "We recommend that the Department of Trade and Industry (DTI) change the rules on business-to-business 'cold calling', they should take the opportunity to explicitly ban the sending of spam to business addresses."

Enforcement Problems

The All Party Internet Group further criticizes the regulation for its lack of enforcement and penalties: "We recommend that the DTI urgently review the ability of the Information Commissioner to police the new Regulations on the sending of spam and provide appropriate powers to deal with what will inevitably be rapidly changing situations."

"The second problem with the UK law is that the agency charged with enforcing it (Information Commissioner) has already indicated that the enforcement provisions may be too weak to be useful to them." Rollo adds.

Troy Rollo

The cost
of spam
in Australia
is in excess of
\$2 billion AUD
per year.

The Spam Act 2003

Laws in Australia Regulating Spam

The Spam Act 2003 is designed to tackle the proliferation of unsolicited e-mails and other messages such as SMS text, used by marketers that not only clog-up consumers inboxes and slow productivity, but often carry offensive and illegal content such as pornography and financial scams. The cost of spam in Australia is in excess of \$2 billion AUD per year.

While the new Spam Act 2003 is unlikely to have much of an impact on the bulk of spam, which originates overseas, it will have consequences for organizations that send e-mails and other electronic messages for commercial purposes.

The Spam Act 2003 received Royal Assent on the 12th of December 2003 and the operative provisions of the Act will take effect 120 days on the 10th of April 2004

Opt-In Regime

The Spam Act 2003 establishes an opt-in regime for commercial electronic messages based on the principle of consent of the receiver unless there is an existing customer-business relationship.

Spam Act 2003 in Detail

Part 2 of the Spam Act 2003 contains specific rules about sending Commercial Electronic Messages

Unsolicited commercial electronic messages

A person must not send, or cause to be sent, a commercial electronic message that has an Australian link and is not a designated commercial electronic message.

Commercial electronic messages must include accurate sender information:

- The message must clearly and accurately identify the individual or organisation who authorised the sending of the message;
- The message must include accurate information about how the recipient can readily contact that individual or organisation;
- The information contained within the message must be valid for at least 30 days after the message is sent.

Commercial electronic messages must contain a functional unsubscribe facility:

- A statement must be made in a clear and conspicuous manner giving directions to allow the recipient to send an unsubscribe message to the individual or organisation who authorised the sending of the first-mentioned message;
- The electronic address is capable of receiving the recipient's unsubscribe message and a reasonable number of similar unsubscribe messages sent by other recipients of the same message.

Rules regarding address-harvesting software and harvested-address lists

Section 3 of the Spam Act 2003 outlines the use and or acquisition of address harvesters and address harvested lists:

- Address-harvesting software must not be acquired or used, and;
- Harvested-address lists must not be acquired or used.

Enforcement

Civil penalties under the Act will be assessed according to a sliding scale for repeat offenders. An individual could be liable for up to a total of \$44,000 AUD for contravention on a single day, while an organization could be fined up to \$220,000 AUD in a day. Offenders with a prior record will be penalized up to a maximum of \$220,000 AUD for each day of spamming by an individual, and \$1.1 million AUD per day for organizations.

The Spam Act will be enforced by The Australian Communications Authority (ACA). The Act gives the Australian Communications Authority an investigative and regulatory role in electronic marketing industry.

The Australian Communications Authority Functions - In addition to the ACA - will oversee the following:

- Issue formal warnings and court injunctions;
- Enforce undertaking by originators of commercial e-mail or address-harvesting software;
- Issue formal warnings as well as court injunctions;
- Seek court imposed penalties;
- Issue infringement notices and fines instead of court proceedings;
- Conduct and/or co-ordinate community education programs.

Can The Spam Act 2003 Reduce Spam?

Supporters of the Spam Act 2003 applaud its strict penalties and opt-in Regulation

"The Australian law bans most spam, and does so without a blanket exemption allowing spamming of businesses. It does have exemptions, but these are in one of two categories: prohibitively difficult to exploit for bulk marketing; or targeted at organizations that are likely to refrain from spamming for other reasons. The penalties are large - sufficient to provide a disincentive to any spammer located in Australia - and they are coupled with a provision requiring forfeiture of profits from spam, which makes it clear that spamming can never be profitable in Australia. We are not aware of any Australian spammer whose activities will not be brought to a complete halt under the Australian law. Even moving operations into an offshore company will not let Australian spammers escape the law because it includes a ban on people being "knowingly concerned in" the spam - a legal term that is well tested in Australia and catches anybody knowingly involved in things such as planning, funding, participating in, or providing facilities for, spam. While overseas enforcement is difficult, the law also bans spam to Australia from outside Australia."

Troy Rollo

The greatest concern regarding the Spam Act 2003 is the need for other worldwide anti-spam legislation to be as stringent.

"Legislation in isolation will, in our (National Office for the Information Economy) opinion, have a minimal effect on spam. To have a significant impact it needs to be complemented by an appropriate enforcement mechanisms, cross-border cooperation, consumer and industry education and the implementation of effective technical measures (ISP/desktop/open relays etc)."

Lindsay Barton

Troy Rollo adds that the way the Spam Act 2003 is written may help Australia deal with offshore spammers. "Due to the way the law is written, it may even be possible to enforce the Australian law against international spammers - at least when they send spam to ".au" domains - and obtain the assistance of foreign courts with that enforcement."

Troy Rollo

Can Spam ever be controlled through Legislation?

(The answer to the million e-mail question)

Introduction

Spam has been called "the cancer of electronic commerce" as the laws are currently, they have had little effect in curbing the spread of this cancer.

Can spam ever be controlled through legislation? The experts we consulted said that in order for spam to be controlled several factors must take place before any legislation can be effective:

1. The Legislation must be enforced.
2. A worldwide approach must be implemented.
3. Greater public knowledge
4. Combination approach of legislation plus technology.

Let the penalty fit the crime

Currently a lot of concern still remains over the types of penalties invoked on spammers and who will issue these penalties. "Spam can be controlled through legislation if the legislation is actually enforced. Through mechanisms such as holding accountable the merchants whose goods and services are advertised in the spam, and 'affiliates' who spam under affiliate programs, a sizable dent can be made in the underlying motivations which lead to spam."

Anne P. Mitchell

Neil Schwartzman adds that the penalties need to address the severity of the crime, "laws must be created with penalties varied to cover the severity of the situation, from small fines to punitive damages and jail time, and with several manners of application from private right of action to state-initiated criminal proceedings."

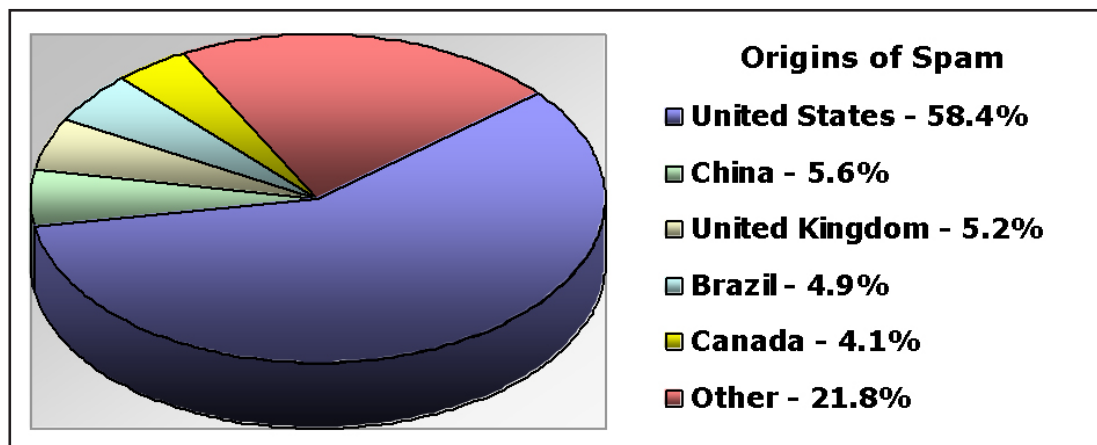
Neil Schwartzman

Worldwide approach

Currently spammers in countries with strict anti-spam legislation can simply move their servers to countries who do not have or have weak spam laws in effect.

Troy Rollo indicates that a worldwide approach is critical if any spam legislation would have any effect. "Spam can be handled, but this does require cooperation from many countries around the world, and requires an opt-in standard with real enforcement of substantial penalties. iCAUCE and related organizations are currently lobbying for such laws in countries covering over 75% of the world's population. Appropriate legislation implemented around the world, can at last reduce spam to a manageable level."

Troy Rollo



Source: The United Nations Conference on Trade and Development (UNCTAD) 2003 E-commerce and development Report

Informed Public

Neil Schwartzman points out that both marketers and consumers must become educated as to proper computing protocols and online community standards. Internet connectivity has constituent responsibilities that have direct positive influence upon other individuals and indeed organizations should they be respected, or conversely negative, should they be ignored "There is no room for naive nor willfully ignorant blunt-force marketing. Furthermore, those with flagrantly exploitable security issues, running a system without a firewall, nor anti-virus and anti-spam protection are invariably hurting others. They must be taught to get their respective houses in order."

Neil Schwartzman

Combined Legislative and Technological Approach

Today e-mails have become the heart and soul of communications for both individuals and enterprises. The use of enforced legislation in combination with advanced anti-spam filters, and blacklist may be the most effective method to control the spread of spam.

"Spam legislation, while well intended, will not control spam alone. The only answer is to fight spammers with the same weapon they use: technology. The problem with spam will be better faced by IT staff than by legislators. To control spam, it must be rendered economically non-viable. Now that is difficult to achieve because it costs virtually nothing to send; however, if we can increase the cost of sending a spam message, we can make it non-viable and the only way we can do that is through the increased use of anti-spam tools".

When anti-spam filters are effective they can eliminate 95% or more of the incoming spam, "...If an anti-spam filter can stop 95% of the spam that reaches an end user, the cost to the spammer of reaching that potential customer has risen by 20 times. Increasing the effectiveness of these filters to 97% increases the cost to the spammer by 33 times. The hope is that the potential revenue available to spammers drops by a corresponding amount, and equilibrium is reached."

Michael D. Osterman

"Legislation is necessary, but is more of an enabler than the "main game". For example ISPs have argued they need legislation to enable them to cost-effectively enforce their AUPs and get spammers taken off-line. Technical measures may stop spam from reaching the intended recipient, but does not make spammers responsible for their actions - legislation can do that. Spammers often claim that their actions are "perfectly legal" - we intend to take away that defense or claim. Spammers have demonstrated quite clearly that they can live with the stigma of doing something that is substantially more repugnant than washing their socks in the town drinking fountain - we can't rely on responsibility or stigma to deter them - ergo legislation.

Despite the necessity of the legislation etc it is really just an interim measure until technical improvements to the underlying SMTP issue 'solves' the problem."

Lindsay Barton

"No legal mechanism is going to eliminate spam - it is just one of the prongs of a necessary multi-pronged approach to dealing with spam. There will always be spammers who operate outside of and beyond the reach of the law, and there must also be technical barriers to spamming along with the legal barriers."

Anne P. Mitchell



About Vircom

For over ten years, Vircom has specialized in the development of advanced Internet Infrastructure server solutions that cater to the demanding messaging and security requirements of two distinct and evolving market segments, namely – enterprises and service providers. With a significant focus on R&D, combined with exceptionally strong client-vendor relations, Vircom products and services continually provide customers with timely, leading edge technology solutions that ensure increased competitiveness, streamlined productivity and a very low Total Cost of Ownership (TCO).

Vircom has become an undeniable force in the anti-spam market with its mature and powerful Modus™ anti-spam technology. Relying on multiple engines and a multi-layered architecture, Vircom's third-generation family of anti-spam solutions, called Modus3™, yield an incomparable catch rate, a very strong false positive protection and the best productivity-enhancing tools for system administrators and network managers.

Built with the robustness required by ISPs and the flexibility corporations look for, Modus™ solutions undoubtedly have the ability to rid your inbox of spam and viruses. Today. Forever.